I CLAIM:

1. A communication system comprising: a communication channel having ends;

at one end of said channel:

(i) a first cipher generator for generating a succession of ciphers, said generator including a first random number generator for generating a sequence of random numbers, each cipher of said succession of ciphers being based on a respective successive portion of said sequence of random numbers; and

(ii) a symmetric encryptor for encrypting successive amounts of information for transmission to the other end of said channel, each amount of information being encrypted using a respective one of said succession of ciphers; and,

at the other end of said channel:

(i) a second cipher generator for generating in synchronism with said first cipher generator the same said succession of ciphers as the first cipher generator, said second cipher generator including a second random number generator for generating the same said sequence of random numbers as said first random number generator; and

(ii) a symmetric decryptor for decrypting the encrypted successive amounts of information received from said one end of said channel, each amount of information being decrypted using the same respective one of said succession of ciphers as was used to encrypt it by said encryptor at said one end of said channel.

2. The system according to claim 1 further comprising:

at said one end of said channel:

(i) means for generating a seed sequence of random numbers, which seed sequence is used by said first random number generator to generate said sequence of random numbers; and

(ii) an asymmetric encryptor for encrypting said seed sequence for transmission over said channel to said other end of the channel; and,

at said other end of said channel:

(i) an asymmetric decryptor for decrypting the encrypted seed sequence received from said one end of the channel, said second random number generator using the decrypted seed sequence to generate said same sequence of random numbers as said first random number generator.

3. The system according to claim 2, wherein said asymmetric encryptor and said asymmetric decryptor employ public key cryptography.

4. The system according to claim 1, wherein a supply to said symmetric encryptor of each of said successive amounts of information, is signalled to both said first and second cipher generators, whereupon the generators synchronously generate the same next cipher in said succession of ciphers.

5. The system according to claim 1, wherein said symmetric encryptor is a block symmetric encryptor and said symmetric decryptor is a block symmetric decryptor.

6. The system according to claim 1, wherein said first and second cipher generators include:

first switching means for receiving said sequence of random numbers;

a plurality of subsidiary cipher generators, said first switching means switching said successive portions of said sequence of random numbers between said plurality of subsidiary cipher generators, each cipher generated by a subsidiary cipher generator being based on a respective said random number sequence portion switched to it by said first switching means; and

second switching means for switching in turn between said subsidiary cipher generators to provide said succession of ciphers.

7. The system according to claim 6, wherein said plurality of subsidiary cipher generators is two subsidiary cipher generators, and said first and second switching means switch simultaneously but to different ones of said two subsidiary cipher generators.

8. The system according to claim 6, wherein each said subsidiary cipher generator comprises:

third switching means;

a plurality of exclusive OR (XOR) gates, said third switching means switching random numbers received by the subsidiary cipher generator between said plurality of XOR gates; and

a plurality of registers, one in respect of each XOR gate, each register both receiving the output of, and providing a further input to, its respective XOR gate, the contents of said plurality of registers constituting the cipher generated by the subsidiary cipher generator.

9. A communication method comprising the steps of:

at one end of a communication channel:

(i) generating a first sequence of random numbers;

(ii) generating a succession of ciphers, each cipher being based on a respective successive portion of said first sequence of random numbers; and

(iii) symmetrically encrypting successive amounts of information for transmission to the other end of said channel, each amount of information being encrypted using a respective one of said succession of ciphers; and,

at the other end of said channel:

(i) generating the same said first sequence of random numbers;

(ii) in synchronism with the generation of said succession of ciphers at said one end of said channel, generating the same said succession of ciphers at said other end of the channel; and

(iii) symmetrically decrypting the encrypted successive amounts of information received from said one end of said channel, each amount of information being decrypted using the same respective one of said succession of ciphers as was used to encrypt it at said one end of said channel.

10. The method according to claim 9, further comprising the steps of:

at said one end of said channel:

(i) generating a seed sequence of random numbers, which seed sequence is used to generate said first sequence of random numbers; and

(ii) asymmetrically encrypting said seed sequence for transmission to said other end of said channel; and,

at said other end of said channel:

(i) asymmetrically decrypting the encrypted seed sequence received from said one end of the channel, the decrypted seed sequence being used to generate said same said first sequence of random numbers.

11. The method according to claim 10, wherein said asymmetric encryption and said asymmetric decryption employ public key cryptography.

12. The method according to claim 9, wherein a supply for symmetric encryption of each of said successive amounts of information, is signalled, whereupon there is the synchronous generation at each end of said channel of the same next cipher in said succession of ciphers.

13. The method according to claim 9, wherein said symmetric encryption is block symmetric encryption and said symmetric decryption is block symmetric decryption.

14. A cipher generator for generating a succession of ciphers, said generator comprising:

a random number generator for generating a sequence of random numbers;

first switching means for receiving said sequence of random numbers;

a plurality of subsidiary cipher generators, said first switching means switching successive portions of said sequence of random numbers between said plurality of subsidiary cipher generators, each cipher generated by a subsidiary cipher generator being based on a respective said random number sequence portion switched to it by said first switching means; and

second switching means for switching in turn between said subsidiary cipher generators to provide said succession of ciphers.

15. The generator according to claim 14, wherein said plurality of subsidiary cipher generators is two subsidiary cipher generators, and said first and second switching means switch simultaneously but to different ones of said two subsidiary cipher generators.

16. The generator according to claim 14, wherein each said subsidiary cipher generator comprises:

third switching means;

a plurality of exclusive OR (XOR) gates, said third switching means switching random numbers received by the subsidiary cipher generator between said plurality of XOR gates; and

a plurality of registers, one in respect of each XOR gate, each register both receiving the output of, and providing a further input to, its respective XOR gate, the contents of said plurality of registers constituting the cipher generated by the subsidiary cipher generator.